METHOD AND DEVICE OF MANIPULATING DATA IN FINITE FIELDS

FIELD OF THE INVENTION

[001] The present invention relates to computations in finite fields, and to conversion between representations of finite fields.

BACKGROUND

[002] Advanced Encryption Standard (AES) provides a Rijndael Block Cipher Algorithm ("the Rijndael algorithm"), which includes a ByteSub bit level operation on an input byte, x. The ByteSub operation includes an encryption mode and a decryption mode. The encryption mode includes a combination of an inverse operation and an affine transformation, e.g., x is converted into $Ax^{-1}+b$, wherein A and b are predetermined parameters. The decryption mode includes a combination of an affine transformation followed by an inverse operation, e.g., x is transformed into $(A^{-1}(x+b))^{-1}$. According to the AES, the inverse operation is preformed over a Galois Field, GF(2^8). The field is represented by a polynomial form, using a reduction polynomial, $p(t)=t^8+t^4+t^3+t+1$.

[003] There are other known block cipher algorithms, which implement an inversion operation in the GF(2^8). These algorithms include, for example, a Camelia cipher algorithm described by *K. Aoki et al.* in *"Specification of Camellia – a 128-bit Block Cipher", http://info.isl.ntt.co.jp/camellia/*, and a Zodiac cipher algorithm described by C. H. Lee in *"Zodiac: Block Cipher Proposal"*, http://www.safedigm.com/productpds/download/Safedigm_Zodiac.pdf.

[004] One method of the AES implements two lookup tables, also referred to as S-boxes, each including 256 values corresponding to 256 possible x values when using the GF(2^8). An encryption S-box includes 256 values of $Ax^{-1}+b$ and a decryption S-box includes 256 values of $(A^{-1}(x+b))^{-1}$. Another method of the AES implements one table, denoted $F(x)$, including 256 values of the inverse of x, namely, x^{-1}. This method requires storage of one table containing 256 values, as well as additional circuitry for implementing the encrypt/decrypt affine transformations, i.e. by multiplying x by A or

A^{-1} and adding b. Thus, the overall conventional implementation of the AES S-box with the set of computations defined by the Rijndael algorithm is not sufficiently efficient.

[005] Designing a more efficient S-box may significantly reduce the complexity of AES implementations, since a conventional hardware implementation of AES requires several, e.g. sixteen, S-boxes.

[006] In *V. Rijmen, "Efficient implementation of the Rijndael S-box"*, http://www.esat.kuleuven.ac.be/~rijmen/rijndael/sbox.pdf ("the Rijmen reference"), it is suggested that using a set of computations based on a representation of $GF(2^8)$ as an expansion of $GF(2^4)$ may improve the efficiency of an AES S-box. However, the Rijmen reference does not disclose, suggest or imply how such a representation might be achieved. Furthermore, the Rijmen reference concludes that even if an AES S-box based on an expanded $GF(2^4)$ could be implemented, such implementation may have no practical use if a good VHDL compiler is used. Therefore, the Rijmen reference teaches away from seeking ways to implement an AES S-box based on an expanded $GF(2^4)$.

SUMMARY OF THE INVENTION

[007] Embodiments of the invention provide a method and a device for efficiently manipulating data provided in a GF(2^{2s}) representation, e.g., for implementing at least some AES encryption and/or decryption operations on data provided in a GF(2^{2s}) representation, by converting the GF(2^{2s}) data into a GF($(2^s)^2$) representation and performing GF(2^{2s}) equivalent operations in the GF($(2^s)^2$) representation.

[008] Exemplary embodiments of the invention may solve a fundamental problem of implementing an AES S-box based on an expanded $GF(2^4)$, for example, an inherent problem of efficiently translating the data from a $GF(2^8)$ representation into a GF($(2^4)^2$) representation, such that the overall procedure of the translation and the operations is more efficient than the conventional implementation.

[009] The method of manipulating data, in accordance with embodiments of the invention, may include converting the GF(2^{2s}) data into corresponding data in a GF($(2^s)^2$) representation. This may be achieved by applying to the GF(2^{2s}) data a conversion operator related to a pre-determined representation-transformation from the GF(2^{2s}) representation to the GF($(2^s)^2$) representation. For example, the conversion operator may include a combination of a linear transformation and the predetermined representation-transformation. In some embodiments the conversion operator may only be related to the representation-transformation. The conversion operator may include a representation-transformation matrix corresponding to the desired transformation. The representation-transformation matrix may be selected from a set of possible representation-transformation matrices according to desired criteria, e.g. minimum area for circuit implementation. Each matrix of the set of matrices may be defined by two field generators, i.e., a root of an irreducible polynomial over the GF(2^{2s}) representation, and a field generator of the GF($(2^s)^2$) representation. The GF($(2^s)^2$) representation may be defined by an irreducible reduction polynomial over GF(2^s) and an extension polynomial over GF(2^s), e.g., an irreducible polynomial of a second degree over GF(2^s).

[0010] According to some embodiments, the method may also include performing on the GF($(2^s)^2$) data at least one operation equivalent to at least one desired operation in the GF(2^{2s}) representation, to provide processed GF($(2^s)^2$) data. The method may also include converting the processed GF($(2^s)^2$) data back into the GF(2^{2s})

representation. This may be achieved by applying to the processed GF($(2^5)^2$) data a de-conversion operator related to the pre-determined representation-transformation. For example, the de-conversion operator may include applying a combination of a linear transformation and an inverse of the predetermined representation-transformation.

[0011] According to some embodiments of the invention there is provided a method for determining the representation-transformation matrix. The method may include synthesizing, e.g., by constructing and/or simulating, a plurality of circuits, each corresponding to a representation-transformation matrix from the GF(2^{2s}) representation into the GF($(2^s)^2$) representation, and/or to an inverse of the representation-transformation matrix. The method may also include selecting one of the matrices based on predetermined optimized criteria, e.g. minimal circuit area.

[0012] According to some exemplary embodiments of the present invention, a method, a system and a device for performing at least some AES S-box encryption and/or decryption operations are provided. According to some exemplary embodiments of the present invention, GF(2^8) input data to be encrypted and/or decrypted by an AES device may be converted from a $GF(2^8)$ representation into data in a GF($(2^4)^2$) representation. According to some embodiments, the conversion may include a linear transformation and/or a predetermined representation-transformation from the $GF(2^8)$ representation into the GF($(2^4)^2$) representation. $GF(2^4)$ operations, equivalent to the $GF(2^8)$ AES encryption/decryption operations may be performed on the GF($(2^4)^2$) data to provide processed GF($(2^4)^2$) data. The processed GF($(2^4)^2$) data may then be converted back into the $GF(2^8)$ representation. According to these embodiments the hardware implementation of the overall process, e.g., the process of converting the data into the GF($(2^4)^2$) representation, performing the equivalent encryption/decryption operations and converting the processed data back into the GF(2^8) representation, may be significantly more efficient than in a conventional hardware implementation of the AES S-box.

[0013] According to further exemplary embodiments of the present invention, there is provided a secure memory storage device compliant with an AES S-box. The storage device may include an input conversion module adapted to convert GF(2^8) data

to be stored into a $GF((2^4)^2)$ representation. The input conversion module may include decryption conversion circuitry and encryption conversion circuitry. The storage device may further include an operations-module adapted to perform operations on the $GF((2^4)^2)$ data and provide processed $GF((2^4)^2)$ data. The operations to be preformed by the operations module may be equivalent to the $GF(2^8)$ AES encryption/decryption operations. The storage device may further include an output de-conversion module adapted to convert the processed $GF((2^4)^2)$ data back into the $GF(2^8)$ representation. The output conversion module may include decryption de-conversion circuitry and encryption de-conversion circuitry.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanied drawings in which:

[0015] Fig. 1 is a flow chart illustration of a method of manipulating data, in accordance with embodiments of the invention;

[0016] FIG. 2 is a schematic illustration of a circuit implementing an AES S-box for encryption and/or decryption of data, according to some exemplary embodiments of the present invention; and

[0017] Fig. 3 is a schematic illustration of an operation module, according to further exemplary embodiments of the invention.

[0018] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn accurately or to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity or several physical components included in one element. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements. It will be appreciated that these

figures present examples of embodiments of the present invention and are not intended to limit the scope of the invention.

DETAILED DESCRIPTION OF THE PRESENT INVENTION

[0019] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, and components have not been described in detail so as not to obscure the present invention.

[0020] In the following detailed description, the notation $GF(2^{2s})$ refers to a representation of a Galois Field (GF) of order 2^{2s} as an extension field of $GF(2)$ consisting a plurality of polynomials over $GF(2)$ modulo $p(t)$, wherein $p(t)$ is an irreducible polynomial of the degree $2s$ over GF(2). A polynomial may be represented in the $GF(2^{2s})$ representation, by a string of $2s$ bits. An element, x, in the $GF(2^{2s})$ representation may be defined by a 2s-digit binary number $x=[x_{2s-1}x_{2s-2}\dots x_1x_0]$, wherein x_i is the coefficient of t^i in a corresponding polynomial, e.g. $x_{2s-1}t^{2s-1}+x_{2s-2}t^{2s-2}+\dots+x_1t+x_0$.

[0021] The notation $GF((2^s)^2)$ refers to a representation of a GF of order 2^{2s} as an extension field of $GF(2^s)$ consisting of a plurality of polynomials over $GF(2^s)$ modulo $r(t)$, wherein $r(t)$ is an irreducible polynomial of a second degree over $GF(2^s)$; i.e., $r(t)=t^2+\alpha t+\beta$, wherein α and β are elements of $GF(2^s)$. The $GF(2^s)$ is represented as an extension field of GF(2) consisting of a plurality of polynomials over GF(2) modulo q(t), wherein q(t) is an irreducible polynomial of the degree s over GF(2). An element, z, in the $GF((2^s)^2)$ representation may be defined by a 2s-digit binary number $z=[z_{2s-1}z_{2s-2}\dots z_1z_0]$ representing a linear polynomial $z_{<m>}t+z_{<l>}$, wherein $z_{<m>}=[z_{2s-1}\dots z_{s+1}z_s]$ and $z_{<l>}=[z_{s-1}\dots z_1z_0]$ are elements of $GF(2^s)$ represented by polynomials modulo q(t).

[0022] Reference is made to Fig. 1, which schematically illustrates a flow chart of a method of manipulating data, in accordance with embodiments of the invention.

[0023] As indicated at block 102, the method may include converting data in a $GF(2^{2s})$ representation into corresponding data in a $GF((2^s)^2)$ representation, which

corresponds to an extension of $GF(2^{2s})$, by applying to the $GF(2^{2s})$ data a conversion operator, as described in detail below.

[0024] As indicated at block 104, the method may also include performing on the $GF((2^s)^2)$ data at least one operation equivalent to at least one desired operation in the $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data, as described in detail below.

[0025] As indicated in block 106, the method may further include converting the processed $GF((2^s)^2)$ data back into the $GF(2^{2s})$ representation, as described in detail below.

[0026] According to some embodiments of the invention, the $GF(2^{2s})$ data may include two or more data blocks. According to these embodiments, the method may be implemented to perform on the two or more data blocks at least one operation in the $GF((2^s)^2)$ representation equivalent to at least one desired operation in the $GF(2^{2s})$ representation.

[0027] According to some exemplary embodiments, the method may be used as part of encrypting and/or decrypting of input data, for example, by performing at least some AES S-box encryption/decryption operations, as described below.

[0028] Although the scope of the present invention is not limited in this respect, for clarity, as part of the description of some embodiments of the present invention, reference may be made to a device and/or a method of encrypting data. Further embodiments of the present invention may be described with reference to a device and/or a method of decrypting data. However, it would be obvious to those with ordinary skills in the art how to modify the methods and/or devices, described below, for both encryption and decryption or the combination of thereof, unless specifically stated otherwise.

[0029] In some exemplary embodiments of the invention, s equals four. These embodiments are useful for converting data in a $GF(2^8)$ representation into corresponding data in a $GF((2^4)^2)$ representation.

[0030] Although the scope of the present invention is not limited in this respect, for clarity, the description of some exemplary embodiments of the present invention

relates to methods and/or devices wherein s equals four, i.e., for converting data in a $GF(2^8)$ representation into a $GF((2^4)^2)$ representation. However, it would be obvious to those with ordinary skills in the art how to accordingly modify the methods and/or devices described below for any other suitable value of s. According to some embodiments of the invention, for some values of s, the conversion from the $GF(2^{2s})$ representation into the $GF((2^s)^2)$ representation may be performed in stages or recursively, e.g., by applying one or more intermediate conversion operators, as described below.

[0031] According to some exemplary embodiments of the invention, the method may be used for performing at least some AES S-box encryption operations wherein s equals four. In these embodiments, the input data to be encrypted may be converted from an extended GF representation, e.g., $GF(2^8)$, into a new representation, e.g., $GF((2^4)^2)$, corresponding to an extension of $GF(2^4)$, as described below. According to these exemplary embodiments, $GF(2^4)$ operations, which may be effectively equivalent to corresponding AES operations in $GF(2^8)$, may be performed on the $GF((2^4)^2)$ data, significantly reducing the complexity level of the calculations. The processed data may then be converted back into the AES $GF(2^8)$ representation, as described below.

[0032] Although some discussions of some embodiments of the present invention may be directed towards the implementation of conversion operators for converting input data, x, from the $GF(2^{2s})$ representation into the $GF((2^s)^2)$ representation, e.g., using specific electrical circuits, it should be understood that the present invention is not limited in this respect. Rather, as part of some embodiments of the present invention, the conversion operator and other operations and processes described below may also be embodied in various other implementations, including implementations known in the present or yet to be devised in the future, for example, any suitable hardware and/or software implementations.

[0033] As part of some embodiments of the present invention, the method may be implemented in a variety of combinations and adaptations. According to an exemplary embodiment of the present invention, an encryption block to perform encryption, and/or a decryption block to perform decryption, may be implemented in

embedded electrical circuitry, e.g., of the type that may be used in a smartcard. The conversion operator that may be used for converting the data to and from the AES $GF(2^8)$ representation to and from the $GF((2^4)^2)$ representation may be pre-programmed, e.g., into a smart card. Other configurations may be used additionally or alternatively.

[0034] According to some exemplary embodiments of the invention, the conversion operator may be related to a representation-transformation from the $GF(2^{2s})$ representation into the $GF((2^s)^2)$ representation. The conversion operator may be related to a representation-transformation matrix corresponding to the representation-transformation. The representation-transformation matrix may be selected from a set of possible representation-transformation matrices according to desired criteria, e.g. minimum area for circuit implementation, as described below. Each matrix of the set of matrices may be defined by a root of an irreducible polynomial over the $GF(2^{2s})$, e.g., $GF(2^8)$, and by a generator of the field extension of the $GF((2^s)^2)$, e.g., $GF((2^4)^2)$ representation, as described below.

[0035] Polynomial representations of $GF(2^4)$ over $GF(2)$ may be defined by each of three irreducible reduction polynomials over $GF(2^4)$, e.g., $1+t+t^4$, $1+t^3+t^4$, $1+t+t^2+t^3+t^4$.

[0036] According to embodiments of the invention, field extensions of one or more of the polynomial representations of $GF(2^4)$ in $GF(2^8)$ may be computed using irreducible extension polynomials, e.g., polynomials of the type $t^2+\alpha t+\beta$, wherein β and α may be elements of $GF(2^4)$, such that $t^2+\alpha t+\beta$ is irreducible over $GF(2^4)$, as described below.

[0037] According to exemplary embodiments of the invention, there may be fifteen different β values and 8 different α values providing 120 possible irreducible extension polynomials of the form $t^2+\alpha t+\beta$. The three different reduction polynomials and the 120 irreducible extension polynomials result in 360 different $GF((2^4)^2)$ representations of $GF(2^8)$ as an extension of $GF(2)$.

[0038] According to some exemplary embodiments of the invention, the number of irreducible extension polynomials of the type $t^2+\alpha t+\beta$ may be reduced. This reduction may be accomplished, for example, using only irreducible extension polynomials of the type $t^2+\alpha t+\beta$ for which $\alpha=1$, as described below. Thus, a total number of relevant GF($(2^4)^2$) representations may be reduced from 360 to 24. However, it should be noted that the present invention is not limited in this respect. Moreover, although the description of some embodiments of the present invention may be restricted to the context of using irreducible extension polynomials of the type $t^2+\alpha t+\beta$ wherein $\alpha=1$, it would be apparent to those of ordinary skill in the art how to adapt these methods using any extension polynomials of the type $t^2+\alpha t+\beta$.

[0039] Thus, as part of some exemplary embodiments of the present invention, a total of twenty-four GF($(2^4)^2$) representations may be computed for converting the data from the standard AES representation into the GF($(2^4)^2$) representation. Each of the twenty-four GF($(2^4)^2$) representations may be defined by one of the reduction polynomials over $GF(2^4)$ and one of the extension polynomials, e.g., of the type $t^2+\alpha t+\beta$, wherein $\alpha=1$.

[0040] Since, as is known in the art, any two finite fields of the same size may be isomorphic, an isomorphism may exist between two representations of $GF(2^n)$, denoted Rep_1 and Rep_2, respectively, wherein $n=2s$. Each of the two representations may be a linear space of dimension n over $GF(2)$, and each isomorphism may be a linear transformation between the representations. Thus, as part of some embodiments of the present invention, an nxn binary representation-transformation matrix, *M*, may be computed for transforming, e.g. by matrix multiplication, elements in Rep_1 into corresponding elements in Rep_2. Since the transformation between the two field representations is invertible, an inverse representation-transformation matrix, M^{-1}, may exist for each representation-transformation. An irreducible polynomial, p_0, having n roots may represent Rep_1. Each root of p_0 is a generator of the $GF(2^n)$ and invariant under field isomorphism. Thus, there are n corresponding representation-transformation matrices for each field extension. A pair of corresponding generators of representations Rep_1 and Rep_2 may uniquely determine an isomorphism between Rep_1 and Rep_2, since a

multiplicative group of the $GF(2^n)$ is cyclic. Thus, for a generator, r_1, of Rep_1, and a generator, r_2, of Rep_2, the corresponding representation-transformation matrix, M, must satisfy $Mr_1=r_2$. Since the two field representations are isomorphic, and since r_1 and r_2 are generators of the $GF(2^n)$, the following equation system must be satisfied by M for any k ($k=1\ldots2^n$):

$$M(r_1)^k=(r_2)^k \qquad (1)$$

wherein $(r_i)^k$ denotes field generator r_i raised to the k-th power in representation Rep_i, to produce an element $(r_1)^k$ in representation Rep_i; and wherein field element $(r_1)^k$ in representation Rep_1 may be treated as a vector in a linear space of dimension n over GF(2), and may be multiplied by representation-transformation matrix, M to provide $M(r_1)^k$.

[0041] Equation system 1 includes 2^n linear equations, which may be solved to determine the representation-transformation matrix, M, corresponding to the pair of generators r_1 and r_2. Equation system 1 may include redundant equations, which may be ignored in order to reduce the number of computations. For example, only the first n equations may be used to provide one representation-transformation matrix. Another representation-transformation matrix may be provided by a solution of Equation set 1 using a different pair of generators r_1 and r_2. Thus, there may be n different equation systems corresponding to the n different generators in Rep_2, which are the image of r_1, providing n different representation-transformation matrices from Rep_1 to Rep_2.

[0042] In exemplary embodiments of the invention, each root of the irreducible polynomial over $GF(2^8)$, e.g., $p(t)=t^8+t^4+t^3+t+1$, may be a generator of the $GF(2^8)$ field. Thus, eight possible representation-transformation matrices corresponding to the eight roots of the irreducible polynomial, respectively, may be computed for each field extension of $GF(2^8)$. Therefore, according to these exemplary embodiments, there may be a set of 192 possible representation-transformation matrices, corresponding to the 24 field extensions, wherein $\alpha=1$. According to some embodiments of the present invention, each of the possible representation-transformation matrices may enable transformation from the standard AES representation into a different $GF((2^4)^2)$ representation of $GF(2^8)$ corresponding to a different extension of $GF(2^4)$.

[0043] According to these exemplary embodiments, the input data, x, in the AES representation may be converted into the GF($(2^4)^2$) representation by applying the representation-transformation, e.g., representation-transformation matrix M. An operation x › x^{-1}, denoted $T(x)$, in the GF($(2^4)^2$) representation may be performed on the converted data, e.g., $M\ \ x$. The conversion to GF(2^8), $F(x)$, may be provided by applying an inverse of the representation-transformation, e.g., M^{-1}. Thus, according to exemplary embodiments of the invention, $F(x)$ and $T(M\ \ x)$ may be provided by the following nonlinear equation:

$$F(x) = M^{1}\ \ T(M\ \ x) \qquad (2)$$

[0044] Equation 2 may be rewritten as follows:

$$M\ \ T(x) = F(M\ \ x) \qquad (3)$$

[0045] According to these embodiments, Equation 3 may have eight solutions, representing the eight possible isomorphisms between the two representations, e.g., between the AES GF(2^8) representation and a corresponding GF($(2^4)^2$) representation. An isomorphism between the two representations may be determined by choosing a generator in one representation to be mapped to a specific generator in the other representation, as described above.

[0046] The following is an exemplary list of matrix strings corresponding to the 192 (24 times 8) possible representation-transformation matrices in hexadecimal form, which may be computed as described above:

Reduction polynomial: $t^4 + t + 1$

(a) Extension Polynomial: $t^2 + t + 8$

01 e1 5c 0c af 1b e3 85, 01 e1 5c 0c ae fa bf 89, 01 5c e0 50 a2 02 b8 db, 01 5c e0 50 a3 5e 58 8b, 01 e0 5d b0 f2 04 ad 6f, 01 e0 5d b0 f3 e4 f0 df, 01 5d e1 ed 42 10 a7 92, 01 5d e1 ed 43 4d 46 7f.

(b) Extension Polynomial: $t^2 + t + 9$

01 e1 5c 0c 12 4b 0f d8, 01 e1 5c 0c 13 aa 53 d4, 01 5c e0 50 1e b2 b5 3a, 01 5c e0 50 1f ee 55 6a, 01 e0 5d b0 4e 09 a1 83, 01 e0 5d b0 4f e9 fc 33, 01 5d e1 ed fe 1c 16 72, 01 5d e1 ed ff 41 f7 9f.

(c) Extension Polynomial: $t^2 + t + 10$

01 e1 5c 0c 43 46 0e 39, 01 e1 5c 0c 42 a7 52 35, 01 5c e0 50 ae bf 54 36, 01 5c e0 50 af e3 b4 66, 01 e0 5d b0 a3 58 fd d3, 01 e0 5d b0 a2 b8 a0 63, 01 5d e1 ed f2 ad f6 c2, 01 5d e1 ed f3 f0 17 2f.

(d) Extension Polynomial: $t^2 + t + 11$

01 e1 5c 0c fe 16 e2 64, 01 e1 5c 0c ff f7 be 68, 01 5c e0 50 12 0f 59 d7, 01 5c e0 50 13 53 b9 87, 01 e0 5d b0 1f 55 f1 3f, 01 e0 5d b0 1e b5 ac 8f, 01 5d e1 ed 4e a1 47 22, 01 5d e1 ed 4f fc a6 cf.

(e) Extension Polynomial: $t^2 + t + 12$

01 e1 5c 0c a2 1a 02 d9, 01 e1 5c 0c a3 fb 5e d5, 01 5c e0 50 f3 03 e4 3b, 01 5c e0 50 f2 5f 04 6b, 01 e0 5d b0 43 05 4d 32, 01 e0 5d b0 42 e5 10 82, 01 5d e1 ed ae 11 fa 73, 01 5d e1 ed af 4c 1b 9e.

(f) Extension Polynomial: $t^2 + t + 13$

01 e1 5c 0c 1f 4a ee 84, 01 e1 5c 0c 1e ab b2 88, 01 5c e0 50 4f b3 e9 da, 01 5c e0 50 4e ef 09 8a, 01 e0 5d b0 ff 08 41 de, 01 e0 5d b0 fe e8 1c 6e, 01 5d e1 ed 12 1d 4b 93, 01 5d e1 ed 13 40 aa 7e.

(g) Extension Polynomial: $t^2 + t + 14$

01 e1 5c 0c 4e 47 ef 65, 01 e1 5c 0c 4f a6 b3 69, 01 5c e0 50 ff be 08 d6, 01 5c e0 50 fe e2 e8 86, 01 e0 5d b0 12 59 1d 8e, 01 e0 5d b0 13 b9 40 3e, 01 5d e1 ed 1e ac ab 23, 01 5d e1 ed 1f f1 4a ce.

(h) Extension Polynomial: $t^2 + t + 15$

01 e1 5c 0c f3 17 03 38, 01 e1 5c 0c f2 f6 5f 34, 01 5c e0 50 43 0e 05 37, 01 5c e0 50 42 52 e5 67, 01 e0 5d b0 ae 54 11 62, 01 e0 5d b0 af b4 4c d2, 01 5d e1 ed a2 a0 1a c3, 01 5d e1 ed a3 fd fb 2e.

Reduction polynomial: $t^4 + t^3 + 1$

(a) Extension Polynomial: $t^2 + t + 2$

01 b1 ec 0c 4f 7c 80 69, 01 b1 ec 0c 4e cd 6c 65, 01 ec 0d 50 ff 60 97 d6, 01 ec 0d 50 fe 8c 9a 86, 01 0d 51 b0 13 c7 94 3e, 01 0d 51 b0 12 ca c5 8e, 01 51 b1 ed 1e 24 91 23, 01 51 b1 ed 1f 75 20 ce.

(b) Extension Polynomial: $t^2 + t + 3$

01 b1 ec 0c f3 2c dc 38, 01 b1 ec 0c f2 9d 30 34, 01 ec 0d 50 43 3c 7a 37, 01 ec 0d 50 42 d0 77 67, 01 0d 51 b0 ae 27 98 62, 01 0d 51 b0 af 2a c9 d2, 01 51 b1 ed a3 28 70 2e, 01 51 b1 ed a2 79 c1 c3.

(c) Extension Polynomial: $t^2 + t + 4$

01 b1 ec 0c ff 21 60 68, 01 b1 ec 0c fe 90 8c 64, 01 ec 0d 50 13 6d c7 87, 01 ec 0d 50 12 81 ca d7, 01 0d 51 b0 1e 96 24 8f, 01 0d 51 b0 1f 9b 75 3f, 01 51 b1 ed 4f 95 7c cf, 01 51 b1 ed 4e c4 cd 22.

(d) Extension Polynomial: $t^2 + t + 5$

01 b1 ec 0c 43 71 3c 39, 01 b1 ec 0c 42 c0 d0 35, 01 ec 0d 50 af 31 2a 66, 01 ec 0d 50 ae dd 27 36, 01 0d 51 b0 a3 76 28 d3, 01 0d 51 b0 a2 7b 79 63, 01 51 b1 ed f2 99 9d c2, 01 51 b1 ed f3 c8 2c 2f.

(e) Extension Polynomial: $t^2 + t + 8$

01 b1 ec 0c af 7d 31 85, 01 b1 ec 0c ae cc dd 89, 01 ec 0d 50 a2 61 7b db, 01 ec 0d 50 a3 8d 76 8b, 01 0d 51 b0 f2 c6 99 6f, 01 0d 51 b0 f3 cb c8 df, 01 51 b1 ed 42 25 c0 92, 01 51 b1 ed 43 74 71 7f.

(f) Extension Polynomial: $t^2 + t + 9$

01 b1 ec 0c 13 2d 6d d4, 01 b1 ec 0c 12 9c 81 d8, 01 ec 0d 50 1e 3d 96 3a, 01 ec 0d 50 1f d1 9b 6a, 01 0d 51 b0 4f 26 95 33, 01 0d 51 b0 4e 2b c4 83, 01 51 b1 ed ff 29 21 9f, 01 51 b1 ed fe 78 90 72.

(g) Extension Polynomial: $t^2 + t + 14$

01 b1 ec 0c 1f 20 d1 84, 01 b1 ec 0c 1e 91 3d 88, 01 ec 0d 50 4e 6c 2b 8a, 01 ec 0d 50 4f 80 26 da, 01 0d 51 b0 ff 97 29 de, 01 0d 51 b0 fe 9a 78 6e, 01 51 b1 ed 13 94 2d 7e, 01 51 b1 ed 12 c5 9c 93.

(h) Extension Polynomial: $t^2 + t + 15$

01 b1 ec 0c a3 70 8d d5, 01 b1 ec 0c a2 c1 61 d9, 01 ec 0d 50 f2 30 c6 6b, 01 ec 0d 50 f3 dc cb 3b, 01 0d 51 b0 42 77 25 82, 01 0d 51 b0 43 7a 74 32, 01 51 b1 ed ae 98 cc 73, 01 51 b1 ed af c9 7d 9e.

Reduction polynomial: $t^4 + t^3 + t^2 + t + 1$

(a) Extension Polynomial: $t^2 + t + 2$

01 50 b0 0c a3 8b d3 d5, 01 50 b0 0c a2 db 63 d9, 01 b0 ed 50 f2 6f c2 6b, 01 b0 ed 50 f3 df 2f 3b, 01 ed 0c b0 43 7f 39 32, 01 ed 0c b0 42 92 35 82, 01 0c 50 ed af 85 66 9e, 01 0c 50 ed ae 89 36 73.

(b) Extension Polynomial: $t^2 + t + 3$

01 50 b0 0c 1e 3a 8f 88, 01 50 b0 0c 1f 6a 3f 84, 01 b0 ed 50 4f 33 cf da, 01 b0 ed 50 4e 83 22 8a, 01 ed 0c b0 fe 72 64 6e, 01 ed 0c b0 ff 9f 68 de, 01 0c 50 ed 13 d4 87 7e, 01 0c 50 ed 12 d8 d7 93.

(c) Extension Polynomial: $t^2 + t + 4$

01 50 b0 0c f3 3b df 38, 01 50 b0 0c f2 6b 6f 34, 01 b0 ed 50 43 32 7f 37, 01 b0 ed 50 42 82 92 67, 01 ed 0c b0 ae 73 89 62, 01 ed 0c b0 af 9e 85 d2, 01 0c 50 ed a3 d5 8b 2e, 01 0c 50 ed a2 d9 db c3.

(d) Extension Polynomial: $t^2 + t + 5$

01 50 b0 0c 4e 8a 83 65, 01 50 b0 0c 4f da 33 69, 01 b0 ed 50 fe 6e 72 86, 01 b0 ed 50 ff de 9f d6, 01 ed 0c b0 13 7e d4 3e, 01 ed 0c b0 12 93 d8 8e, 01 0c 50 ed 1f 84 6a ce, 01 0c 50 ed 1e 88 3a 23.

(e) Extension Polynomial: $t^2 + t + 8$

01 50 b0 0c ae 36 62 89, 01 50 b0 0c af 66 d2 85, 01 b0 ed 50 a2 63 c3 db, 01 b0 ed 50 a3 d3 2e 8b, 01 ed 0c b0 f3 2f 38 df, 01 ed 0c b0 f2 c2 34 6f, 01 0c 50 ed 42 35 67 92, 01 0c 50 ed 43 39 37 7f.

(f) Extension Polynomial: $t^2 + t + 9$

01 50 b0 0c 13 87 3e d4, 01 50 b0 0c 12 d7 8e d8, 01 b0 ed 50 1f 3f ce 6a, 01 b0 ed 50 1e 8f 23 3a, 01 ed 0c b0 4e 22 65 83, 01 ed 0c b0 4f cf 69 33, 01 0c 50 ed fe 64 86 72, 01 0c 50 ed ff 68 d6 9f.

(g) Extension Polynomial: $t^2 + t + 14$

01 50 b0 0c fe 86 6e 64, 01 50 b0 0c ff d6 de 68, 01 b0 ed 50 13 3e 7e 87, 01 b0 ed 50 12 8e 93 d7, 01 ed 0c b0 1e 23 88 8f, 01 ed 0c b0 1f ce 84 3f, 01 0c 50 ed 4e 65 8a 22, 01 0c 50 ed 4f 69 da cf.

(h) Extension Polynomial: $t^2 + t + 15$

01 50 b0 0c 43 37 32 39, 01 50 b0 0c 42 67 82 35, 01 b0 ed 50 ae 62 73 36, 01 b0 ed 50 af d2 9e 66, 01 ed 0c b0 a3 2e d5 d3, 01 ed 0c b0 a2 c3 d9 63, 01 0c 50 ed f2 34 6b c2, 01 0c 50 ed f3 38 3b 2f.

[0047] The above list is organized such that each group of 8 matrix string values is associated with one of the 8 extension polynomials of the type $t^2 + \alpha t + \beta$ and one of the three irreducible reduction polynomials over $GF(2^4)$, as described above. The matrix string values are listed in the form of 8 pairs of values in hexadecimal form, representing an 8×8 binary matrix. In order to locate the values corresponding to the *i-th* *M* representation-transformation matrix in the list, wherein $1 \le i \le 192$, the following set of equations may be solved:

$$i - 1 = Q1 \times 64 + R1 \qquad (4)$$

$$R1 = Q2 \times 8 + R2$$

wherein:

$$0 \le R1 \le 64 \qquad (5)$$

$$0 \le R2 < 8$$

[0048] Equation set 4 with the boundary conditions of Equation set 5 may yield a set of the values *Q1, Q2, R1, R2* corresponding to a desired *i-th* representation-transformation matrix. The location of a desired representation-transformation matrix, e.g. the *i-th* matrix in the above list may be defined by the *Q1+1* reduction polynomial, the *Q2+1* extension polynomial, and the *R2+1* matrix string. The matrix string values may be converted into the transformation matrix representation, by separating the matrix string into pairs of numbers in hexadecimal form. Each column of the transformation matrix may then be represented

using the binary representation of a corresponding hexadecimal pair, e.g., using eight binary digits.

[0049] Some embodiments of the present invention include an AES compatible S-box. The AES compatible S-box may be configured to perform AES S-box equivalent operations, e.g., encryption and or decryption operations, over the $GF((2^5)^2)$ representation. The AES compatible S-box may include, for example, conversion circuitry enabling the conversion of data from the standard AES S-box based representation into the $GF((2^5)^2)$ representation, as described above. The AES compatible S-box may also include an operations module, which may include operation circuitry and/or software to process the converted data, e.g. to perform AES equivalent operations on the converted data. The AES compatible S-box may also include de-conversion circuitry to convert the processed data back into the AES representation.

[0050] A conventional AES S-box may perform affine transformations according to the following equations:

$$sbox[x] = A \times F[x] \oplus b \qquad (6)$$

$$sbox^{-1}[x] = F[A^{-1} \times (x \oplus b)] \qquad (7)$$

wherein A and b are AES S-box parameter matrices, as is known in the art.

[0051] Thus, according to embodiments of the invention, substituting Equation 3 in Equations 6 and 7, respectively, may yield the following equations to convert x into the $GF((2^5)^2)$ representation, perform operations in the $GF((2^5)^2)$ representation, and convert the resulting data back into corresponding data in the AES representation:

$$sbox[x] = AM \times T[M^{-1} \times x] \oplus b \qquad (8)$$

$$sbox^{-1}[x] = M\,T[(AM)^{-1} \times (x \oplus b)] \qquad (9)$$

[0052] In accordance with some embodiments of the present invention, the conversion circuitry or software may include circuitry implementing the representation-transformation matrix M. According to some of these embodiments, the circuitry or software implementing the representation-transformation matrix M may be combined with the circuitry or software implementing a linear transformation, for example, AES S-Box parameters, e.g., A. According to further embodiments of the invention, the conversion circuitry or software may include four multiplication modules,

e.g., as described below, for multiplication by $M, AM, M^{-1}, and (AM^{-1})$, respectively. Thus, the conversion circuitry may consist of a combination of applying a linear transformation and the predetermined representation-transformation. For example the conversion circuitry may implement the addition of AES S-box parameter b, e.g. by a XOR circuit, to provide the sum $x+b$, which may further be multiplied by an inverse of AM. The conversion circuitry may implement other combinations of a linear transformation and the representation-transformation matrix, e.g., the specific implementations described herein. The use of such operation modules may enhance the efficiency of the conversion circuitry.

[0053] A hardware implementation of matrix multiplication may include any hardware implementation of matrix multiplication, as is known in the art. For example, values y_i of a block y defined by $y=Dx$, wherein $i=1...8$ and wherein D is a fixed 8×8 binary matrix, may be computed using the following equation:

(6)

$$y_i = \sum_{j=1}^{8} D_{i,j} x_j \qquad (10)$$

[0054] Thus, values of y may be computed using Equation 10. This may be achieved by determining which of the elements of row $D_{i,j}$ are nonzero and performing a XOR operation of the corresponding values of x_j.

[0055] According to exemplary embodiments of the invention, operations, e.g. inverse, adding, and/or multiplication operations, equivalent to AES operations may be defined in the new representation, as described below.

[0056] An element x of a GF(2^8) may be defined by an eight-digit binary number $x=[x_7x_6x_5x_4x_3x_2x_1x_0]$, and an element z of a GF(2^4) may be defined by a four-digit binary number $z=[z_3z_2z_1z_0]$.

[0057] As is known in the art, GF(2^4) may have a polynomial representation defined by a reduction polynomial over GF(2), e.g., $z=[z_3z_2z_1z_0]$ may be represented by the polynomial $z_0+z_1t+z_2t^2+z_3t^3$. Multiplication of elements in the GF may be defined by multiplying the polynomials representing the elements and reducing the result modulo the reduction polynomial. In the following description, an inverse operation x^{-1} of x in

the AES GF(2^8) may be denoted $F=F(x)$, and an inverse operation z^{-1} of z in the new representation may be denoted $T=T(z)$.

[0058] According to embodiments of the invention, a bit octet, $z=[z_7z_6z_5z_4z_3z_2z{\cdot}z_0]$, of GF($2^8$) may be analogous to a linear polynomial $z_{<m>}t+z_{<l>}$, wherein $z_{<m>}=[z_7z_6z_5z_4]$ and $z_{<l>}=[z_3z_2z_1z_0]$ are elements of GF(2^4). Thus, the new representation may include elements $z_{<m>}$ and $z_{<l>}$ of GF(2^4).

[0059] As part of some embodiments of the present invention, multiplication and addition operations in the new representation may be defined in terms of operations on $GF(2^4)$. Provided below is one possible definition of multiplication and addition in the new representation in terms of operations over $GF(2^4)$. It will be appreciated that other definitions may also be used as part of some embodiments of the present invention.

[0060] Addition and subtraction of two elements, e.g., $a,d \in GF(2^8)$, in the new representation may be defined as a bitwise XOR of the two elements, as is known in the art. The product of the two elements, a and d, may be defined as a polynomial product $(a_{<m>}t + a_{<l>}) \times (d_{<m>}t + d_{<l>}) \bmod (t^2 + \alpha t + \beta)$, wherein multiplication and addition of the polynomial coefficients may be defined by operations over $GF(2^4)$ using a given representation. Thus, the product of elements a and d may be calculated using the following equation:

$$\begin{aligned}&(a_{<m>}t + a_{<l>}) \times (d_{<m>}t + d_{<l>})(\text{mod } t^2 + \alpha t + \beta) = \\ &(a_{<l>}d_{<m>} - a_{<m>}d_{<m>}\alpha + a_{<m>}d_{<l>})t - a_{<m>}d_{<m>}\beta + a_{<l>}d_{<l>} \equiv r_{<m>}t + r_{<l>}\end{aligned} \tag{11}$$

wherein:

$$\begin{aligned}&(a_{<l>}d_{<m>} - a_{<m>}d_{<m>}\alpha + a_{<m>}d_{<l>}) \equiv r_{<m>} \equiv [r_7r_6r_5r_4] \\ &a_{<m>}d_{<m>}\beta + a_{<l>}d_{<l>} \equiv r_{<l>} \equiv [r_3r_{2r_1}r_0]\end{aligned} \tag{12}$$

[0061] Thus, the product of elements a and d in the AES $GF(2^8)$ may be defined as $r=[r_7r_6r_5r_4r_3r_2r_1r_0]$.

[0062] Determining an inverse $x^{-1}=(c_{<m>}t + c_{<l>})$ of data element $x=(a_{<m>}t + a_{<l>})$, may require $(x_{<m>}x + x_{<l>})$ solving the following set of equations:

$$0x+1=(c_{<m>}t+c_{<l>})\times(a_{<m>}t+a_{<l>})=$$
$$0x+1=(c_{<m>}t+c_{<l>})\times(a_{<m>}t+a_{<l>})\bmod(t^2+\alpha t+\beta)= \qquad (13)$$
$$0x+1=(c_{<m>}a_{<m>}\alpha+c_{<m>}a_{<l>}+c_{<l>}a_{<m>})t+c_{<l>}a_{<l>}+c_{<m>}a_{<m>}\beta$$

[0063] Equation set 13 may be translated into the following system of liner equations over $GF(2)$:

$$\begin{aligned} c_{<m>} &= a_{<m>}(a^2_{<m>}\beta+a^2_{<l>}+a_{<l>}a_{<m>}\alpha)^{-1} \\ c_{<l>} &= (a_{<l>}+a_{<m>}\alpha)(a^2_{<m>}\beta+a^2_{<l>}+a_{<l>}a_{<m>}\alpha)^{-1} \end{aligned} \qquad (14)$$

[0064] Thus, in order to calculate an inverse x^{-1} of data element x, the values of $C_{<m>}$ and $C_{<l>}$ may be calculated, as described above.

[0065] According to embodiments of the invention, a direct computation of Equation system 14 may require two square computations, e.g., $a^2_{<m>}$ and $a^2_{<l>}$, five multiplication computations, one inversion and three additions, all taken over $GF(2^4)$. However, as part of some embodiments of the present invention, the number of these computations may be reduced, as explained below.

[0066] According to embodiments of the invention, additions over $GF(2^4)$ may be implemented as XOR circuits, as is known in the art. According to other embodiments of the invention, the multiplication over $GF(2^4)$ may be performed more efficiently by defining $GF(2^4)$ multipliers and selecting the appropriate multiplier in each case, as explained below.

[0067] According to these exemplary embodiments, a multiplication $a \times d = [a_3, a_2, a_1, a_0] \times [d_3, d_2, d_1, d_0]$ over $GF(2^4)$, of two elements, e.g., $a = [a_3, a_2, a_1, a_0]$ and $b = [d_3, d_2, d_1, d_0]$, of $GF(2^4)$, may be defined as a sequence of bitwise operations, e.g., additions (XOR) and multiplications (AND), for a given reduction polynomial, e.g., as described above. Thus, the solutions of the multiplication of two elements may be as follows:

<u>Reduction polynomial: $t^4 + t + 1$</u>

$[a_3,a_2,a_1,a_0]$ * $[d_3,d_2,d_1,d_0]$ =

$[a_1d_2+a_3d_3+a_3d_0+a_2d_1+a_0d_3, a_2d_3+a_0d_2+a_3d_3+a_2d_0+a_1d_1+d_2a_3,$
$a_1d_3+d_2a_3+a_0d_1+a_2d_2+a_2d_3+a_1d_0+a_3d_1, a_0d_0+a_1d_3+a_2d_2+a_3d_1]$

Reduction polynomial: $t^4 + t^3 + 1$

$[a_3,a_2,a_1,a_0] * [d_3,d_2,d_1,d_0] =$

$a_0d_3+a_1d_3+a_3d_2+a_2d_3+a_3d_1+a_2d_1+a_1d_2+a_3d_3+a_3d_0+a_2d_2, a_0d_2+a_3d_3+a_1d_1+a_2d_0, a_0d_1+a_3d_2+a_3d_3+a_1d_0+a_2d_3, a_1d_3+a_0d_0+a_2d_3+a_3d_2+a_2d_2+a_3d_1+a_3d_3]$

Reduction polynomial: $t^4 + t^3 + t^2 + t + 1$

$[a_3,a_2,a_1,a_0] * [d_3,d_2,d_1,d_0] =$

$[a_2d_1+a_3d_0+a_3d_1+a_1d_2+a_1d_3+a_2d_2+a_0d_3, a_3d_1+a_2d_2+a_1d_1+a_2d_0+a_0d_2+a_1d_3,$
$a_0d_1+a_1d_3+a_1d_0+a_3d_1+a_3d_3+a_2d_2, a_3d_2+a_1d_3+a_0d_0+a_2d_3+a_2d_2+a_3d_1]$

[0068] It may be noted that some of the multiplications of elements in each of the solutions are similar for two or more output bits. For example, the expression $a_1d_3+a_2d_2+a_3d_1$, appearing twice in the solutions listed above, may be computed only once in order to minimize hardware requirements, e.g., using XOR and AND gates. It will be appreciated by those skilled in the art, that the solutions for multiplication of two elements in $GF(2^4)$ using each of the three quadratic reduction polynomials discussed above may be used to construct a $GF(2^4)$ multiplier for each of the quadratic reduction polynomials. Such multiplier may be implemented in hardware and/or software as is known in the art. An appropriate $GF(2^4)$ multiplier may be constructed for a given representation-transformation matrix. Since each representation-transformation matrix may be defined by one of the three irreducible reduction polynomials over $GF(2^4)$ in combination with an extension polynomial, as described above, the $GF(2^4)$ multipliers may be predetermined. It may be appreciated by a person skilled in the art that other suitable implementations of $GF(2^4)$ multipliers may be used additionally or alternatively in accordance with exemplary embodiments of the invention.

[0069] Inversion, denoted *INV*, and squaring, denoted *SQR*, in $GF(2^4)$ may be implemented by two respective, relatively small, Look-Up-Tables (LUTs) having a size of 8-bytes each, e.g., 16 nibbles. According to some embodiments of the present

invention, coefficient β may be predetermined. Thus, the value $\beta \times g^2$ for an element $g \in GF(2^4)$ may also be stored in an 8-byte LUT, which may be denoted βSQR, thereby eliminating one multiplication from the set of computations required for computing Equation System 14. According to alternative embodiments, *SQR*, *INV* and/or β SQR in $GF(2^4)$ may be implemented by any suitable circuit, as is known in the art. For example, an *SQR* circuit may be implemented by substituting a=d in the solutions for multiplication of two elements, as described above. Thus, the *SQR* circuits may implement the following solutions:

<u>Reduction polynomial: $t^4 + t + 1$</u>

$[a_3,a_2,a_1,a_0]^2 = [a_3, a_1+a_3, a_2, a_0+a_2]$

<u>Reduction polynomial: $t^4 + t^3 + 1$</u>

$[a_3,a_2,a_1,a_0]^2 = [a_2+a_3, a_1+a_3, a_3, a_0+a_2+a_3]$

<u>Reduction polynomial: $t^4 + t^3 + t^2 + t + 1$</u>

$[a_3,a_2,a_1,a_0]^2 = [a_2, a_1+a_2, a_2+a_3, a_0+a_2]$

[0070] It may be noted that the circuitry implementation of embodiments of the invention, may be more compact than the corresponding LUT implementation. However, in some S-box implementations, a LUT may provide more efficient processing of the data.

[0071] According to exemplary embodiments of the invention, the 129th representation-transformation matrix, i.e. the matrix having the hexadecimal notation *M=01,50,b0,0c,a3,8b,d3,d5*, may be selected from the 192 representation-transformation matrices listed above. Thus, the corresponding extension reduction polynomials are $p(t) = t^4 + t^3 + t^2 + t + 1$, and $r(t) = t^2 + t + 2$, *i.e.* $\beta=2$. According to this exemplary embodiment, the multiplication circuit is $[a_3,a_2,a_1,a_0]*[d_3,d_2,d_1,d_0]=[a_2d_1+a_3d_0+a_3d_1+a_1d_2+a_1d_3+a_2d_2+a_0d_3, a_3d_1+a_2d_2+a_1d_1+a_2d_0+a_0d_2+a_1d_3, a_0d_1+a_1d_3+a_1d_0+a_3d_1+a_3d_3+a_2d_2, a_3d_2+a_1d_3+a_0d_0+a_2d_3+a_2d_2+a_3d_1]$.

[0072] According to this exemplary embodiment of the invention, the following LUTs, listed in hexadecimal notation, may be used to calculate respective values of *SQR*, βSQR and/or *INV* corresponding to an input number, *l*, between 0 and 15:

SQR=0,1,4,5,f,e,b,a,2,3,6,7,d,c,9,8 (15)

βSQR=0,2,8,a,1,3,9,b,4,6,c,e,5,7,d,f

INV=0,1,f,a,8,6,5,9,4,7,3,e,d,c,b,2

wherein the output of each table may be the *l-th* entry of the table. Alternatively, SQR, *βSQR* and/or INV may be calculated using the circuit implementation, as described above, e.g. the *SQR* circuit is provided by $[a_3,a_2,a_1,a_0]^2 = [a_2, a_1+a_2, a_2+a_3, a_0+a_2]$

[0073] Reference is made to FIG. 2, which illustrates a circuit implementation of an AES compatible S-box 200 for encrypting/decrypting data, in accordance with some exemplary embodiments of the present invention.

[0074] S-box 200 may be implemented to provide an output *sbox[x]* or $sbox^{-1}[x]$ corresponding to the block data *x* according to Equations 8 and 9, as described below.

[0075] S-box 200 may include an input conversion module 221 to receive the input data, *x*, in AES representation, e.g., including 8-bit data, denoted $x = [x_7x_6x_5x_4x_3x_2x_1x_0]$ $(x \in GF(2^8))$, and to apply a conversion operator to convert this data into data in the $GF((2^4)^2)$ representation, as described above. In the decrypt mode of operation, conversion module 221 may also apply the decrypt affine transformation to *x*, as described below. S-box 200 may also include an operation module 230 to process the converted data, e.g. by performing $GF(2^8)$ equivalent encryption/decryption operations, and to provide processed $GF((2^4)^2)$ data, as described below. S-box 200 may also include an output de-conversion module 223, to convert the processed data back into the AES representation, as described below. Module 223 may also apply the encrypt affine transformation to the output of module 230, as described below.

[0076] According to these exemplary embodiments, module 221 may include a first data input path 202 corresponding to an encryption mode of operation, i.e., to perform the conversion *sbox[x]*, as described above. Module 221 may also include a second data input path 204 corresponding to a decryption mode of operation, i.e. to perform the conversion $sbox^{-1}[x]$.

[0077] According to exemplary embodiments of the invention, module 221 may include encryption conversion circuitry 214, and decryption conversion circuitry 210. Circuitry 214 may include an M^{-1} multiplier adapted to apply a conversion operator to *x*,

e.g., to implement multiplication of x by M^{-1}. Circuitry 210 may be adapted to apply a conversion operator to x, e.g., circuitry 210 may include a XOR module 216 for implementing a XOR operation of x with b, and an $(AM)^{-1}$ multiplier 218 to implement multiplication of the output of module 216 by $(AM)^{-1}$. Thus, the output of circuitry 214 may be $M^{-1}x$, corresponding to the expression in brackets of Equation 8. The output of circuitry 210 may be $(AM)^{-1} \times (x \oplus b)$, corresponding to the expression in brackets of Equation 9.

[0078] According to exemplary embodiments of the invention, module 221 may also include a multiplexer 220, which may have two inputs associated with the outputs of circuits 214 and 210, respectively. Multiplexer 220 may be used to select between these two inputs, such that an output of multiplexer 220 may include one output of converted data 231 corresponding to the selected input. Multiplexer 220 may include any suitable circuitry known in the art for selection between two inputs. For example, multiplexer 220 may include a control register (not shown). The control register may store an indication bit to indicate the required mode of operation, e.g., the indication bit may equal zero for the encrypt mode of operation and may equal one for the decrypt mode of operation. The output of multiplexer 220 may be selected according to the value of the indication bit, as is known in the art. The value of the indication bit may be set before performing an encryption or a decryption operation on a plurality of data blocks. Converted $GF((2^4)^2)$ data 231 may include 8 bits carried, for example, by eight parallel electric conductors (not shown), as is known in the art. The eight conductors may be separated into two sets of four conductors, respectively. Thus, the eight bits of converted data 231 may be split into two 4-bit data values $z_{<m>} = [z_7 z_6 z_5 z_4]$, denoted 235, and $z_{<l>} = [z_3 z_2 z_1 z_0]$ ($z_{<m>}, z_{<l>} \in GF(2^4)$), denoted 231, corresponding to the values of the eight bits of converted data 231, as described above.

[0079] Module 230 may include circuitry, as described below, to process data values $z_{<m>}$ and $z_{<l>}$ and provide processed data represented by $T(x) = c_{<m>}t + c_{<l>}$, as described above. The values of $c_{<m>}$ and $c_{<l>}$ may be provided by Equation system 14, wherein $z_{<m>}$ and $z_{<l>}$ are substituted for $a_{<m>}$ and $a_{<l>}$, and wherein $\alpha = 1$.

[0080] According to exemplary embodiments of the invention, operation module 230 may include operation circuitry for performing AES equivalent operations on

converted data 231, as described above. The operation circuitry may include a first 8 bitwise XOR box 232 and a second 8 bitwise XOR box 234. The operation circuitry may also include three copies, 236, 238 and 240 of the $GF(2^4)$ multiplier, as described above. The operation circuitry may also include three circuits/8-byte tables implementing *INV* 242, *SQR* 244 and *βSQR* 246, respectively, as described above. Circuits/tables 242, 244 and 246 and multipliers 236, 238, and 240 may be predetermined according to the selected reduction polynomial, as described above. Thus, the respective outputs $c_{<l>}$ *and* $c_{<m>}$, of multipliers 240 and 238, may equal $(z_{<l>}+z_{<m>})(z^2_{<m>}\beta+ z^2_{<l>}+z_{<l>}z_{<m>})^{-1}$ and $z_{<m>}(z^2_{<m>}\beta+ z^2_{<l>}+z_{<l>}z_{<m>})^{-1}$, respectively.

[0081] The four bit output of multiplier 240 and the four bit output of multiplier 238 may be re-combined at the output of module 230 to form one eight-bit data output corresponding to the operation, *T*, performed on converted data 231. Thus, in the encryption mode of operation the output of module 230 may include the value of $T[M^{-1} \times x]$ according to Equation 8. In the decryption mode of operation, the output of module 230 may include the value of $T[(AM)^{-1} \times (x \oplus b)]$ according to Equation 9. The eight-bit output of module 230 may be received by module 223.

[0082] Module 223 may include a first data path 272 corresponding to an encryption mode of operation, and a second data path 274 corresponding to a decryption mode of operation. Module 223 may include encryption de-conversion circuitry 285, and decryption de-conversion circuitry 282. Circuitry 282 may include an *M* multiplier associated with path 272. Multiplier 282 may be used in the decryption mode to convert the processed $GF((2^4)^2)$ data back into the AES representation, e.g., to provide $MT[(AM)^{-1} \times (x \oplus b)]$ in accordance with Equation 9. . Circuitry 285 may include an *AM* multiplier 284 associated with path 274, and a XOR block 286 associated with an output of multiplier 284. Multiplier 284 may be used in combination with XOR block 286 to convert the processed $GF((2^4)^2)$ data back into the AES representation in the encryption mode of operation, e.g., to provide $AM \times T[M^{-1} \times x] \oplus b$, in accordance with Equation 8. According to exemplary embodiments of the invention, module 223 may also include a multiplexer 290, which may have two inputs associated with outputs of XOR block 286 and multiplier 282, respectively. Multiplexer 290 may be used to select between these two inputs, such that an output of multiplexer 290 may include one

output corresponding to the mode of operation. Multiplexer 290 may include any suitable circuitry known in the art for selection between two inputs. For example, multiplexer 290 may include circuitry similar to the circuitry of multiplexer 220, as described above.

[0083] Examples of the operation of S-box 200 are provided below. A first example demonstrates encrypting data using an AES compliant S-box, in accordance with an embodiment of the present invention. A second example demonstrates decryption of data according to other exemplary embodiments. In the examples provided, the 129^{Th} representation-transformation matrix from the set of matrices listed above is used, and the input data, x, is chosen to have a value of 67. It should be noted that the representation-transformation matrix and the input data in these examples have been randomly selected for demonstrative purposes only and are not intended to limit the scope of the invention to any particular choice of representation-transformation matrix or to any specific input data value.

[0084] Initially, the input data, in this exemplary embodiment represented by the hexadecimal value 67 ($T1$), may be loaded through input path 202. The input data may be multiplied by M^{1} at multiplier 214, resulting in 2e ($T3$). Next, T3 is input to multiplexer 220, which is set at the encryption mode. Thus, T3 is then split into two 4-bit values, namely, $T7 = 2$ and $T6 = e$. The two 4-bit values are then XORed at XOR box 232, yielding $T11 = T6 \oplus T7 = c$. $T7$ is input to βSQR circuit/table 246 resulting in $T10 = 2 \cdot 2^2 = 8$. Multiplier 236 is used to produce $T9 = T7 \cdot T6 = 2 \cdot e = 3$, according to the multipliers described above. T6 is also input to SQR circuit/table 244 resulting in $T8 = e^2 = 9$. The values $T8$, $T9$ and $T10$ are XORed at XOR box 234 producing $T12 = T8 \oplus T9 \oplus T10 = 2$. $T12$ is then input to INV circuit/table 242 resulting in $T13 = T12^{-1} = f$. Multiplier 238 receives inputs $T11$ and $T13$, and multiplier 240 receives inputs $T7$ and $T13$, resulting in $T14 = T11 \cdot T13 = 6$, and $T15 = T7 \cdot T13 = 1$. Next, $T15$ and $T14$ are combined to produce a single 8-bit data value, i.e. $T16=16$. The single 8-bit data value is input to multiplier 284 resulting in $T18 = (AM) \cdot 16 = e6$. Finally, $T18$ is XORed at XOR box 286 with b producing $T19 = T18 \oplus b = 85$. Multiplexer 258 chooses $T20 = T19 = 85$ as the output. Thus, The output, $sbox[x]$, of the S-box is 85.

[0085] Provided below is an example of utilizing the S-box to decrypt the (encrypted) output of the S-box described in the previous example. The S-box is initially input with the data value $T1 = 85$. $T1$ is XORed at box 216 with b resulting in $T2 = T1 \oplus b = e6$. T2 is multiplied by $(AM)^{-1}$ at multiplier 218 to produce $T4 = (AM)^{-1} \cdot e6 = 16$. Then, $T4$ is selected by multiplexer 220 (set to the decryption mode) to receive $T5$. $T5$ is split into $T6 = 6$ and $T7 = 1$. The two 4-bit values are then XORed at box 232, yielding $T11 = T6 \oplus T7 = 7$. Next, using circuits/tables β-SQR 246, SQR 244 and multiplier 236, values $T10 = \beta \cdot T7^2 = 2$, $T9 = T6 \cdot T7 = 6$, and $T8 = T6^2 = b$ are calculated. The outputs of T8, $T9$ and $T10$ are XORed at box 234 resulting in $T12 = T8 \oplus T9 \oplus T10 = f$. $T12$ is then input to INV table 242 resulting in $T13 = T12^{-1} = 2$. Multiplier 238 has an input of $T11$ and $T13$, and multiplier 240 has an input of $T7$ and $T13$. The resulting output of multipliers 240 and 238 is $T14 = T11 \cdot T13 = e$, and $T15 = T7 \cdot T13 = 2$, respectively. Next, $T14$ and $T15$ are combined to produce a single 8-bit data value $T16 = 2e$. $T16$ is multiplied by M at multiplier 582 to produce $T17 = M \cdot 2e = 67$. Finally, multiplexer 290 selects the output $T20 = T17 = 67$.

[0086] Reference is made to Fig. 3, which schematically illustrates an operation module 330, according to further exemplary embodiments of the invention.

[0087] According to some exemplary embodiments of the invention module 230 (Fig. 2) of S-box 200 (Fig. 2) may be replaced by module 330 to allow performing the AES equivalent operations for $\alpha \neq 1$. Module 330 may include an alpha multiplier 332 to multiply value 235 by α. The output of multiplier 332 may be provided as inputs to XOR block 232 and multiplier 236, respectively. Thus, the $c_{<m>}$ output of multiplier 238 and the $c_{<l>}$ output of multiplier 240 may be provided according to Equation set 14, as described above.

[0088] According to some embodiments of the invention there is provided a method for determining the representation-transformation matrix from the set of representation-transformation. The method may include synthesizing, e.g. by constructing and/or simulating, a plurality of circuits, each corresponding to a representation-transformation matrix from the $GF(2^{2s})$ representation into the $GF((2^s)^2)$ representation, as described above. The method may also include selecting one of the

matrices based on predetermined optimized criteria, e.g. minimal circuit area, as described below.

[0089] According to exemplary embodiments of the invention, each representation-transformation matrix M of the set of possible representation-transformation matrices, e.g. the 192 representation-transformation matrices discussed above, may be implemented to provide conversion from the AES representation into the $GF((2^4)^2)$ representation, as described above. Each representation-transformation matrix may be implemented by an appropriate electrical circuit, e.g., as described above, and/or appropriate software process, and may have different performance characteristics, as discussed below. Thus, according to embodiments of the invention, a representation-transformation matrix may be selected from the set of matrices according to any desired criteria, as described below.

[0090] According to embodiments of the invention, the operation parameters under which the circuits are tested may affect the relative results of the circuits. Thus the optimality of a circuit or process may depend on the operation parameters used, as described below. Furthermore, the determination of a circuit or process as being optimal may also depend on the criteria used to evaluate the circuits/processes. Thus, different circuits/processes may be determined to be optimal for different operation parameters and/or criteria, as described below.

[0091] According to some exemplary embodiments of the invention, the comparison criteria may include the number of gates and/or power consumption required by each of the circuits/processes to convert the sample data and to perform the AES equivalent operations described above. According to other embodiments of the invention, any other desired optimization criteria may be applied.

[0092] According to exemplary embodiments of the invention, a set of circuits, e.g. 192 circuits, corresponding to the 192 possible transformation matrices, respectively, may be fabricated, e.g. corresponding to s-box 200 (Fig. 2) described above. According to these exemplary embodiments, each one of the circuits may be synthesized using a DC Shell 2001.08-sp1 (DC Expert) available from Synopsis. A target library TSMC 0.18μ (SAAG-X Artisane) may be used. The synthesis may be performed for various timings, e.g., time propagation delays, for example, ranging from

12nSec to *6nSec*. These parameters may enable using different respective frequencies, e.g., in the range of 66.7MHz to 111MHz by adding a margin, for example, a 3-nanosecond margin. According to these exemplary embodiments, the results of the method described above may be summarized by the following table:

Table I

Timing (nSec) (Tpd)	12	10	8	6
Max. Frequency (Mhz)	66.7	76.9	90.9	111.1
Min. Area (μ^2) for option (#)	3948 (82)	4650 (167)	4726 (167)	5495 (124)
Max. Area (μ^2) for option (#)	4480 (45)	5704 (62)	5977 (128)	8236 (128)
Relative Min./Max. % Difference	13	23	26	50

wherein numbers in parentheses denote circuits corresponding to the index number of the representation-transformation matrices, as described above. Thus, for example, for timing=12, the minimal area circuit was obtained when using matrix No. 82, and the maximal area circuit was obtained when using matrix No. 45.

[0093] As may be noted in Table 1, some circuits may appear to be more desirable than others in terms of minimum area required for implementation, as well as in terms of other criteria and/or under certain operation parameters. As may be further noted, the performances of each of the circuits may be dependent upon the operation parameters of the circuit. The modification of certain operation parameters may affect the individual circuits in a generally similar manner. It should be appreciated, however, that some circuits may yield optimal results when operated under certain operation parameters, and significantly non-optimal results when the operation parameters are changed. For example, the area of the circuits may increase with frequency, regardless of the selected representation-transformation matrix; however, for different frequencies, different circuits may provide optimal results, for example, a different optimal area required for implementing the circuits. The differences in performance may be contributable, at least in part, to different levels of complexity of the AES S-box equivalent LUTs and to computations in the $GF((2^4)^2)$representation of $GF(2^8)$ which may differ amongst different circuits and under various operation parameters.

[0094] According to some embodiments of the invention, some of the circuits may be less sensitive to frequency changes and substantially consistently provide better results when operated under various operation parameters. For example, circuits 82, 105, 124 and 128, corresponding to respective equivalent representation-transformation matrices, as described above, may provide desirable results under various operation parameters. The differences in the performances of the various circuits, as well as the desirability of some of the circuits in a substantially large number of cases, may be associated with the use of the three alternatives for the *INV* and *SQR* circuits/tables and the $GF(2^4)$ multiplier, as described above. In addition, different circuits may dictate different βSQR circuits/tables, and the multiplication by $M, AM, M^{-1}, (AM^{-1})$ may also differ, as described above.

[0095] According to further exemplary embodiments of the invention, the conversion from the $GF(2^{2s})$ representation into the $GF((2^s)^2)$ representation may be performed in stages or recursively, e.g., by applying one or more intermediate conversion operators. For example, operations in the $GF(2^s)$ representation wherein *s=2u*, may be analogous to operations in a $GF(2^{2u})$ representation. The operations in the $GF(2^{2u})$ representation may be performed in a $GF((2^u)^2)$ representation. Thus, an intermediate conversion operator may be applied to convert data in the $GF((2^s)^2)$ representation into corresponding data in the $GF((2^u)^2)$ representation. If desired, a second intermediate conversion operator may be applied to convert the data in the $GF(2^u)$ representation into corresponding data in a $GF((2^v)^2)$ representation, wherein *u=2v*, and so on. Thus, operations in a $GF(2^{2^j q})$, wherein q is odd, may be performed using operations in a $GF((..(((2^q)^2)^2)...)^2)$ representation, by using operations in $GF(2^q)$. The conversion from one GF representation to another GF representation, e.g., having half the size, may be designed according to efficiency criteria, e.g., circuitry and/or power efficiency, of specific implementations.

[0096] It will be appreciated by persons skilled in the art that the present invention is not limited to the exemplary embodiments of the invention shown and described herein with reference to the accompanying drawings. While certain features of the invention have been illustrated and described, many modifications, substitutions, changes, and equivalents may occur to those skilled in the art. It is, therefore, to be

understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the invention.